



EUROPEAN PATENT SPECIFICATION

Date of publication of patent specification :
01.02.95 Bulletin 95/05

Int. Cl.⁶ : **H04L 12/46, H04L 12/22**

Application number : **90312060.8**

Date of filing : **02.11.90**

Repeaters for secure local area networks.

Priority : **06.12.89 GB 8927623**

Date of publication of application :
12.06.91 Bulletin 91/24

Publication of the grant of the patent :
01.02.95 Bulletin 95/05

Designated Contracting States :
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

References cited :
GLOBECOM 89 November 1989, IEEE New York US pages 185 - 190; C.K.KWOK et al.: "ON TRANSPARENT BRIDGING OF CSMA/CD NETWORKS" MINI MICRO SYSTEMS. vol. XXII, no. 2, February 1989, BOSTON US pages 86 - 88; J.WEINSTEIN: "BRIDGING TO A BETTER LAN" PATENT ABSTRACTS OF JAPAN vol. 8, no. 167 (E-258)(1604) 02 August 1984, & JP-A-59 63839 (RICOH) 11 April 1984

Proprietor : **3COM IRELAND**
Ugland House
P.O. Box 309
George Town Grand Cayman (KY)

Inventor : **Carter, Steven Howard**
Misbourne,
Perks Lane,
Prestwood
Great Missenden, Bucks HP16 OJD (GB)
Inventor : **Lockyer, Terence Denning**
10 Avebury Avenue
Luton, Bedfordshire LU2 7DT (GB)
Inventor : **Gahan, Christopher John**
50 Belham Road
Kings Langley, Hertfordshire WD4 8BY (GB)

Representative : **Crawford, Andrew Birkby et al**
A.A. THORNTON & CO.
Northumberland House
303-306 High Holborn
London WC1V 7LE (GB)

Note : Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid (Art. 99(1) European patent convention).

Description

This invention relates to local area networks for providing intercommunication between computers and/or other digital equipment (hereinafter called data termination equipment and abbreviated to DTE). More particularly, it is concerned with networks of the kind in which DTE's are connected (normally via a media attachment Unit (MAU), also called a transceiver) to a common transmission medium such as a coaxial cable, a twisted pair cable or an optical fibre and in which digital repeaters (usually multiport repeaters, MPR's) are used to restore digital signals that have been attenuated or otherwise degraded and to provide for branching when required. The invention includes improved repeaters and the networks in which they are used.

The invention is primarily (but not exclusively) concerned with networks operating Carrier Sense Multiple Access techniques with collision detection (CSMA/CD). The best-known networks of this type are those specified by the International Standards Organisation as ISO 8802/3 networks and by Xerox Corporation as "Ethernet" networks.

In such systems, data is transmitted in frames which have a limited range of lengths and are normally made up of a meaningless preamble (for establishing synchronisation), a start-of-frame indicator, a destination address segment, a source address segment, a control segment (indicating, for instance, the frame length), a segment of data (often beginning with a frame or protocol identification) to be transmitted to the DTE identified by the address identification, and a frame check segment for verifying accuracy of transmission.

MPR's repeat frames received on an input port indiscriminately to all their output ports and necessarily (because of delay limits imposed by the network specifications) begin to retransmit before the complete frame has been received.

A local area network as so far described is insecure, in the sense that any DTE can transmit data to any other and that an eavesdropper gaining access to the transmission medium can read all the data.

In known systems, a measure of security may be achieved by physically subdividing the transmission medium into groups using components called "bridges" which receive and store computer data frames and can then analyse them and determine whether they are authorised frames and if so to which of its output ports they need to be re-transmitted. However, bridges are much more expensive than MPR's and introduce a delay in excess of the frame length.

A typical such bridge is described in an article by J. Weinstein in Mini-Micro February 1989 entitled "Bridging to a Better LAN".

A further bridging structure is described by Con-

rad K. Kwok et al in "On Transparent Bridging of CSMA/CD Networks" presented at IEEE Global Telecommunications Conference and Exhibition, Dallas, Texas November 1989. In this article a "cut-through bridge" is described which functions largely like a passive repeater at light loads and largely like a normal bridge at heavy loads. This is achieved by beginning to forward a frame received from a first network to a second network before the complete frame is received. At heavy loads a collision will occur and therefore transmission to the second network cannot be completed. In such a case the frame is buffered by the bridge for transmission later. Also, once the complete destination address of a frame has been received by the bridge, the bridge can determine whether or not that frame needs to be transmitted to the second network according to whether that destination is present in the second network.

The present invention provides a secure repeater for use in a local area network and arranged to be connected, in use, to a plurality of data termination equipment (DTEs), the repeater comprising means for receiving incoming data frames; means for retransmitting said frames during a time interval that begins before a complete frame of data has been receiving; means for storing access rules for the DTEs connected to it; means for reading at least one portion of the frame selected from the destination address segment, the source address segment, the control segment and the frame or protocol identifier, if present, of each incoming data frame and comparing the portion or portions so read with the stored access rules to determine whether the frame is permitted or not; and means for corrupting the frame in retransmission if it determines that it is not.

The present invention thus provides repeaters with security features such that in a local area network in which they are used the expense and signal delay inherent in the use of bridges can be avoided, or at least minimised.

When the portion of the frame selected to be read is in the control segment, it may be the whole segment or it may be only a part of the segment that is relevant to the decision to be made. In most (but not necessarily all) other cases, the whole of the appropriate address segment or of the identifier should be read.

The access rules may be written to their storing means in various ways, depending (among other things) on the level of security required. For example, a degree of security can be achieved by allowing a learning period when the network is first set up in which the repeater "self-learns" which DTE's are connected to each of its ports and thus sets up its own access rules for each port forbidding the transmission thereafter of any frame with a source address not corresponding with a DTE not connected to that port during the learning period.

More sophisticated rules can be loaded (or self-

learned rules can be edited) using data provided as control frames from a network manager, or if the possibility of the network manager being misused or counterfeited needs to be allowed for, from a special input device (a key pad or a mobile memory device, for instance) coupled to the repeater itself and protected from misuse either by password protection or by removing the input device once the access rules have been written. In extreme cases, the means provided in the repeater for coupling the input device could be destroyed after use, or the rules could be inserted as a pre-programmed ROM encapsulated along with key components of the repeater to prevent substitution.

Either one or both of the destination address segment and the source identification segment may be read and compared with the stored access rules, depending on the nature of the rules to be applied. For example, if the physical connections are such that all the DTE's connected to a particular input port (or group of ports) of a repeater have unlimited access to the network, then there is no point in comparing the destination address segments of frames received on that port, and it is only necessary to check the source address segment to verify that the DTE in question is authorised to be connected there. Similarly, if physical security can be relied on to prevent unauthorised connections and all the DTE's connected to a port (or group of ports) have the same (but limited) access to other parts of the network, then only the destination address segment needs to be read and compared.

Subject to the limitations set by comparison time and storage space, each DTE may have its own access rules, independently of all the others, or if the DTE's are organised in groups with common access rules, then it is possible for individual DTE's to be allocated to more than one of the groups; for example, a departmental accountant's terminal could have access to all the other terminals within his department and also to other accountants' terminals outside the department, without the need to give unnecessary access between the remaining terminals of those two groups.

Ideally, all the data contained in an unauthorised frame should be corrupted, and this presents no problems if the destination address segment shows the frame to be unauthorised; if however it is the source address, the control frame or the frame or protocol identifier segment that shows the frame to be unauthorised, the time taken to make comparisons may be such that a few bytes of data may be retransmitted without corruption. If this is considered unacceptable, high-speed comparison algorithms may be used and/or the system protocol may be modified so that there will be an appropriate number of meaningless bytes at the beginning of the data segment.

Data may be corrupted, when required, by overwriting a series of binary digits selected from all 1's,

all 0's, cyclically repeated sequences and pseudo-random sequences. The first two require no more complex generating means than a simple logic gate, say a non-exclusive OR gate, receiving the incoming data on one input and a permitted/not permitted flip-flop signal on its other input so as to pass the data to output if the flipflop is set "permitted" but a continuous "high" or "low" output if it is set "not permitted".

Cyclically repeated or pseudo-random sequences can be read from memory or generated when required by conventional means.

Data may alternatively be corrupted by encrypting it in a manner that cannot be decrypted by the DTE's of the network, except possibly one or a few authorised DTE's (for instance the network controller). This provides the facility for the controller, or a security unit, to be informed of the content of the corrupted frame.

If desired, a repeater which detects an unauthorised frame may, in addition to corrupting it, switch off the port on which such a frame was received and/or the port to which the DTE it was addressed to is connected. Preferably it only does so if it knows that the port concerned is not connected to another repeater.

On occasion, an unauthorised person gaining access to a network may not be concerned to transmit unauthorised data, nor to read data from the network, but to prevent proper functioning of the network. One easy way of so "jamming" a conventional network is to inject into it a rapid succession of frames that conform to the system protocol, so that any other user seeking to transmit will encounter a "collision". As a precaution against this form of abuse, the repeater in accordance with the invention may additionally be fitted with a timer (or frame counter) device arranged to limit the number of consecutive frames that will be accepted on any one port and to switch off that port if the limit is exceeded.

If desired, the repeater in accordance with the invention may be switchable (eg by a local, key-operated switch or by a control frame from a network manager) between secure operation in accordance with the invention and ordinary, insecure, operation; the latter may be desirable, for example, during fault testing and identification.

The invention will be further described by way of example with reference to the accompanying drawings in which Figure 1 is a diagram of a network in accordance with the invention incorporating four multiport repeaters and Figure 2 is a block diagram of those parts of a multiport repeater that are relevant to understanding of the present invention.

The network of Figure 1 comprises 14 items of data termination equipment, DTE 1 to DTE 14 (which may for example be general purpose personal computers, dedicated word processors, printers, disc drives etc), and a network controller C. Each of these is connected through its own media access unit MAU

1 to MAU 15 to one or other of three multiport repeaters MPR 1, MPR 2 and MPR 3; these are in turn interconnected by the remaining repeater MPR 4.

Figure 2 shows one module serving ports 1 to 4 of an MPR, the assumption for the purpose of illustration being that there is at least one other module serving further ports, and that the access rules will be the same for all the ports connected to this module.

The most basic conventional function of the MPR is served by the inputs received on any one of ports 1 to 4 passing via respective port interface units 5 and multiplexers 6 and 7 to a first in/first out memory 8. This is inert until enabled by a signal from a start of frame detector 9, and then begins to store the incoming data. In the meantime, a preamble generator 10 has begun to output a preamble signal through the multiplexer 11 to all of the port interfaces, which will pass it to their respective ports except in the case of the port receiving the incoming signal. Preamble transmission continues until a counter 12 indicates that the prescribed length of preamble has been outputted. Provided there are then at least 3 bits of data in the memory 8, the multiplexer 11 is switched to begin reading out the data stored in the memory, and in the ordinary way will continue to do so until the complete frame has been received into and then read from the memory 8.

However, in accordance with the invention, the incoming signal is also passed via a shift register 13 which extracts the destination address and the source address in parallel form to latches 14 and 15 which are switched by counters 16 enabled by the start of frame signal from detector 9. These are passed to comparators 17 and compared with the access rules previously stored in a database 18.

If the comparators indicate that the frame is not in accordance with the rules contained in the database, then a signal is output via a delay 19 (serving to ensure that the source address will never be corrupted) to the multiplexer 7, and cause it to transmit, for the remainder of the length of the frame, a meaningless sequence of digits available to it from a sequence generator 20 instead of the incoming signal. Preferably when such a signal is given, data is also transmitted to the network controller C identifying the port on which the frame concerned was received, the destination address and source address of the frame and the reason for the decision that the frame was unauthorised. If desired, this signal may be separated from the system data signals into a separate signalling medium, designated on the diagram as an info bus.

The repeater provides in addition conventional facilities for detecting a collision and transmitting jam signals in response to it, for extending signal fragments arising from collisions and for disabling a port on which excessive collisions or frame lengths exceeding the protocol limit are indicative of faulty

equipment.

Suppose, by way of example, that DTE's 1 to 5 need to communicate with each other but with none of the other DTEs. DTE's 6 to 9 similarly need access only to each other but DTE 10 needs access not only to DTE 6 to 9 but also DTEs 11 to 14; obviously, all the DTE's need to be in communication with the network controller C. This could be achieved by connecting MAUs 1 to 5 to one module (or to separate modules with the same instructions in their address rule databases) in MPR 1, MAU 6 to 9 to one module and MAU 10 to a separate module in MPR 2 and similarly MAUs 11 to 14 to one module and MAU 15 to a second module in MPR 3. In MPR 1, the address database needs to be loaded with rules accepting destination addresses corresponding to the network controller C and to its own DTE's 1 to 5 but no other, and may optionally be loaded with the source addresses of its own DTE's 1-5 in order to reject signals from an additional DTE connected to it without authority. The first module of MPR 2 is correspondingly loaded. The second module of MPR 2, on the other hand, is loaded with rules accepting destination addresses corresponding to MAU's 6 to 9 and 11 to 14 as well as to the network controllers MAU 15 (and if required to accept no source address except that of DTE 10).

The first module of MPR 3 is loaded with rules accepting destination addresses corresponding to any of MAU's 10-15 (and optionally to accept only source addresses corresponding to MAU's 11 to 14); and the second module of MPR 3 is loaded to accept any destination address (and preferably to accept no source address except that of the network controller C).

MPR 4 may, if physical security is reliable, be a conventional MPR without security features; or it may be a repeater in accordance with the invention loaded with analogous rules to provide additional security.

Note that in this example, the network has been so arranged that each destination address and each source address is either accepted or rejected unconditionally. This has the advantage of requiring the shortest processing time, and consequently allowing an unauthorised frame to be corrupted from as nearly as possible the beginning of its data segment. It is however possible, subject to process time limitations, to provide conditional rules allowing certain destination addresses to be accessed from some but not all of the DTE's connected to the module in question.

Claims

1. A secure repeater for use in a local area network and arranged to be connected, in use, to a plurality of data termination equipment (DTEs), the repeater comprising means (5,6) for receiving incoming data frames; means (8,11,5) for retransmitting said frames during a time interval that be-

- gins before a complete frame of data has been receiving; means (18) for storing access rules for the DTEs connected to it; means (13,14,15) for reading at least one portion of the frame selected from the destination address segment, the source address segment, the control segment and the frame or protocol identifier, if present, of each incoming data frame and comparing the portion or portions so read with the stored access rules to determine whether the frame is permitted or not; and means (20) for corrupting the frame in retransmission if it determines that it is not.
2. A repeater as claimed in claim 1 including means for reading and comparing both the destination address segment and the source address segment of the incoming frame.
 3. A repeater as claimed in claim 1 or claim 2 in which the said means (20) for corrupting the data frame comprises means for overwriting it with a series of binary digits selected from all 1's, all 0's, cyclically repeated sequences and pseudo-random sequences.
 4. A repeater as claimed in claim 1 or claim 2 in which the means for corrupting the data frame is encrypting means.
 5. A repeater as claimed in any one of the preceding claims in which the said access rules are self-learned on the basis of the identity of equipment connected to its ports during an initial learning period.
 6. a repeater as claimed in any one of claims 1-4 in which the said access rules are written to the repeater by a network manager.
 7. A repeater as claimed in any one of claims 1-4 in which the said access rules are written to the repeater from an input device coupled to it and removed once the acces rules have been written.
 8. A repeater as claimed in any one of claims 1-4 in which the said access rules are written to the repeater by an input device protected from misuse by password protection.
 9. A repeater as claimed in any one of the preceding claims in which, when an unauthorised frame is detected, in addition to the frame being corrupted the port on which it was received, and/or the port to which the DTE it was addressed to is connected, is switched off.
 10. A repeater as claimed in any one of the preceding claims including means for switching off any input

port on which a number of consecutive frames in excess of a predetermined limit are received.

5 Patentansprüche

1. Sicherer Zwischenverstärker zum Einsatz in einem Nahbereichsnetz, der in Funktion mit einer Vielzahl von Datenendeinrichtungen (DTE's) verbunden wird, wobei der Zwischenverstärker eine Einrichtung (5,6) zum Empfang ankommender Datenrahmen umfaßt; eine Einrichtung (8,11,5) zum Weiterübermitteln der Rahmen während eines Zeitabschnitts, der beginnt, bevor ein kompletter Datenrahmen empfangen worden ist; eine Einrichtung (18) zum Speichern von Zugangsregeln für die damit verbundenen DTE's; eine Einrichtung (13,14,15) zum Lesen wenigstens eines Teils des Rahmens, der aus dem Zieladressensegment, dem Ursprungsadressensegment, dem Steuersegment und der Rahmen- oder Protokollkennung - falls vorhanden - jedes ankommenden Datenrahmens ausgewählt worden ist, und zum Vergleichen des so gelesenen Teils bzw. der so gelesenen Teile mit den gespeicherten Zugangsregeln, um festzustellen, ob der Rahmen zugelassen ist oder nicht; sowie eine Einrichtung (20) zum Verstümmeln des Rahmens beim Weiterübermitteln, wenn sie feststellt, daß er es nicht ist.
2. Zwischenverstärker nach Anspruch 1, der eine Einrichtung zum Lesen und Vergleichen sowohl des Zieladressensegments als auch des Ursprungsadressensegments des ankommenden Rahmens enthält.
3. Zwischenverstärker nach Anspruch 1 oder Anspruch 2, wobei die Einrichtung (20) zum Verstümmeln des Datenrahmens eine Einrichtung zum Überschreiben desselben mit einer Reihe von Binärziffern umfaßt, die aus allen Einsen, allen Nullen, zyklisch wiederholten Sequenzen und pseudozufälligen Sequenzen ausgewählt werden.
4. Zwischenverstärker nach Anspruch 1 oder Anspruch 2, wobei die Einrichtung zum Verstümmeln des Datenrahmens eine Verschlüsselungseinrichtung ist.
5. Zwischenverstärker nach einem der vorangehenden Ansprüche, wobei die Zugangsregeln auf der Grundlage der Kennung der mit seinen Kanälen verbundenen Geräte während einer anfänglichen Lernperiode selbst gelernt werden.
6. Zwischenverstärker nach einem der Ansprüche

- 1-4, wobei die Zugangsregeln durch einen Netzmanager in den Zwischenverstärker geschrieben werden.
7. Zwischenverstärker nach einem der Ansprüche 1-4, wobei die Zugangsregeln von einer Eingabevorrichtung in den Zwischenverstärker geschrieben werden, die mit ihm verbunden ist und entfernt wird, wenn die Zugangsregeln eingeschrieben worden sind.
8. Zwischenverstärker nach einem der Ansprüche 1-4, wobei die Zugangsregeln von einer Eingabevorrichtung in den Zwischenverstärker geschrieben werden, die durch Paßwortschutz gegen Mißbrauch geschützt ist.
9. Zwischenverstärker nach einem der vorangehenden Ansprüche, wobei, wenn ein unzulässiger Rahmen erfaßt wird, zusätzlich zur Verstümmelung des Rahmens der Kanal, über den er empfangen wurde, und/oder der Kanal, mit dem die DTE, an die er adressiert war, verbunden ist, abgeschaltet wird.
10. Zwischenverstärker nach einem der vorangehenden Ansprüche, der eine Einrichtung zum Abschalten jedes beliebigen Eingangskanals einschließt, an dem eine Anzahl aufeinanderfolgender Rahmen empfangen wird, die eine vorgegebene Grenze übersteigt.

Revendications

1. Un répéteur protégé pour utilisation dans un réseau de zone locale et agencé afin d'être relié, en utilisation, à une pluralité d'équipements de terminaux de données (DTE), le répéteur comprenant des moyens (5, 6) pour recevoir des blocs de transmission de données arrivant ; des moyens (8, 11, 5) pour retransmettre lesdits blocs de transmission durant un intervalle de temps, qui commence avant qu'un bloc de transmission de données complet ait été reçu ; des moyens (18) pour emmagasiner des règles d'accès pour les équipements de terminaux de données reliés à lui ; des moyens (13, 14, 15) pour lire au moins une partie du bloc de transmission sélectionné à partir du segment d'adresse de destination, le segment d'adresse de source, le segment de commande et le dispositif d'identification de bloc de transmission ou de protocole, si présents, de chaque bloc de transmission de données arrivant, et comparer la partie ou les parties ainsi lues avec les règles d'accès emmagasinées, afin de déterminer si le bloc de transmission est autorisé ou non ; et des moyens (20) pour altérer le

bloc de transmission en retransmission si ils déterminent que c'est non.

2. Un répéteur tel que revendiqué dans la revendication 1, incluant des moyens pour lire et comparer, à la fois, le segment d'adresse de destination et le segment d'adresse de source du bloc de transmission arrivant.
3. Un répéteur tel que revendiqué dans la revendication 1 ou la revendication 2, dans lequel lesdits moyens (20) pour altérer le bloc de transmission de données comprennent des moyens pour le surcharger avec une série de chiffres binaires, ces derniers étant sélectionnés tout avec des 1, tout avec des 0, des séquences répétées cycliquement et des séquences pseudo-aléatoires.
4. Un répéteur tel que revendiqué dans la revendication 1 ou la revendication 2, dans lequel les moyens pour altérer le bloc de transmission de données sont des moyens de cryptage.
5. Un répéteur tel que revendiqué dans une quelconque des précédentes revendications, dans lequel desdites règles d'accès sont auto-apprises sur la base de l'identité d'équipement relié à ces ports durant une période d'apprentissage initial.
6. Un répéteur tel que revendiqué dans une quelconque des revendications 1 à 4, dans lequel lesdites règles d'accès sont écrites au répéteur par un manager de réseau.
7. Un répéteur tel que revendiqué dans une quelconque des revendications 1 à 4, dans lequel lesdites règles d'accès sont écrites au répéteur à partir d'un dispositif d'entrée, couplé à lui et retiré une fois que les règles d'accès ont été écrites.
8. Un répéteur tel que revendiqué dans une quelconque des revendications 1 à 4, dans lequel lesdites règles d'accès sont écrites au répéteur par un dispositif d'entrée, protégé contre un emploi abusif par une protection à mot de passe.
9. Un répéteur tel que revendiqué dans une quelconque des précédentes revendications, dans lequel, lorsque un bloc de transmission non autorisé est détecté, en supplément au bloc de transmission étant altéré, le port sur lequel il était reçu, et/ou le port auquel l'équipement de terminaux de données lui était adressé et relié, sont mis hors service.
10. Un répéteur tel que revendiqué dans une quelconque des précédentes revendications, incluant des moyens pour mettre hors circuit un port d'en-

trée quelconque, sur lequel un nombre de blocs de transmission consécutifs excédant une limite prédéterminée est reçu.

5

10

15

20

25

30

35

40

45

50

55

7

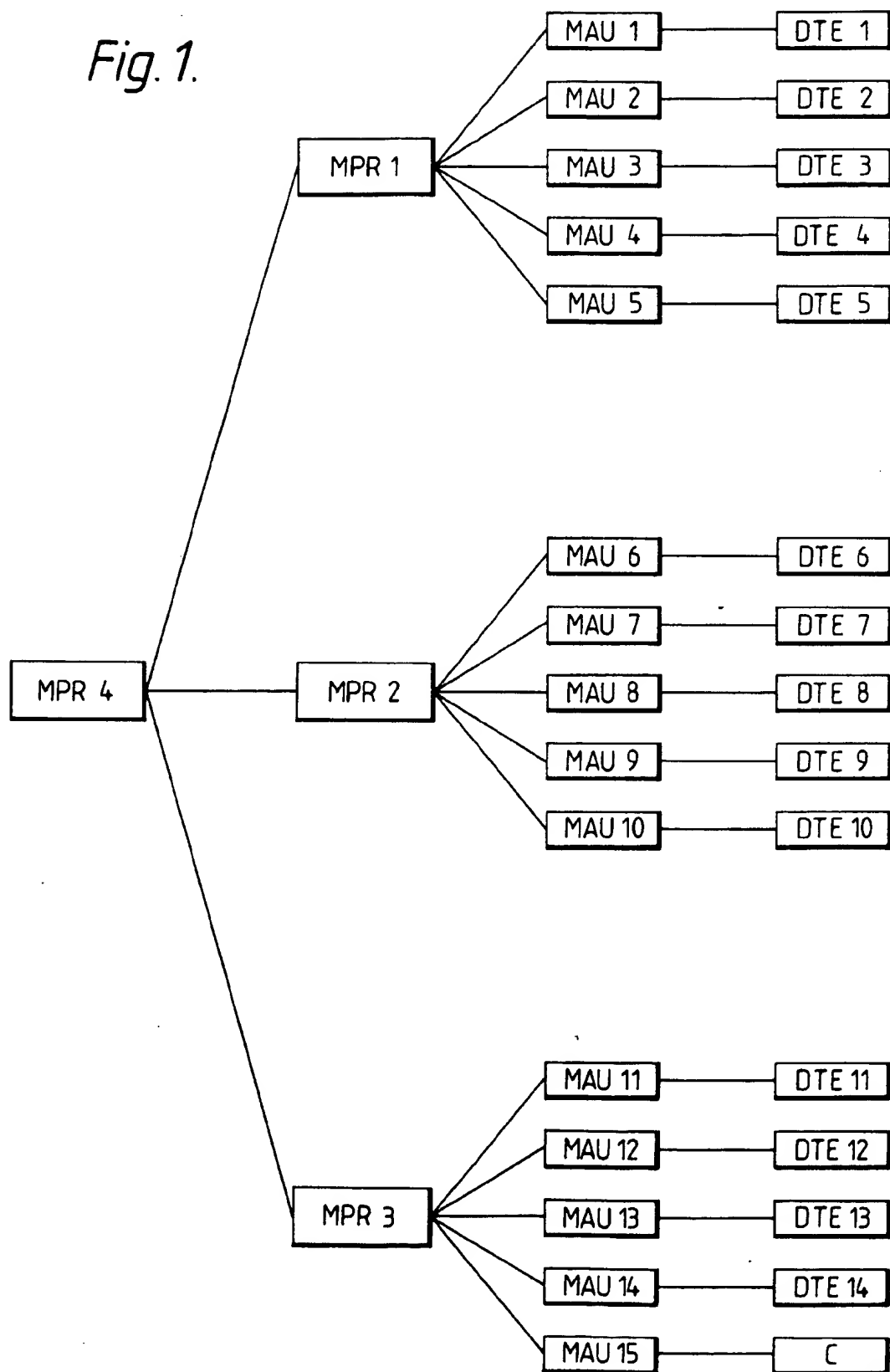
Fig. 1.

Fig. 2.

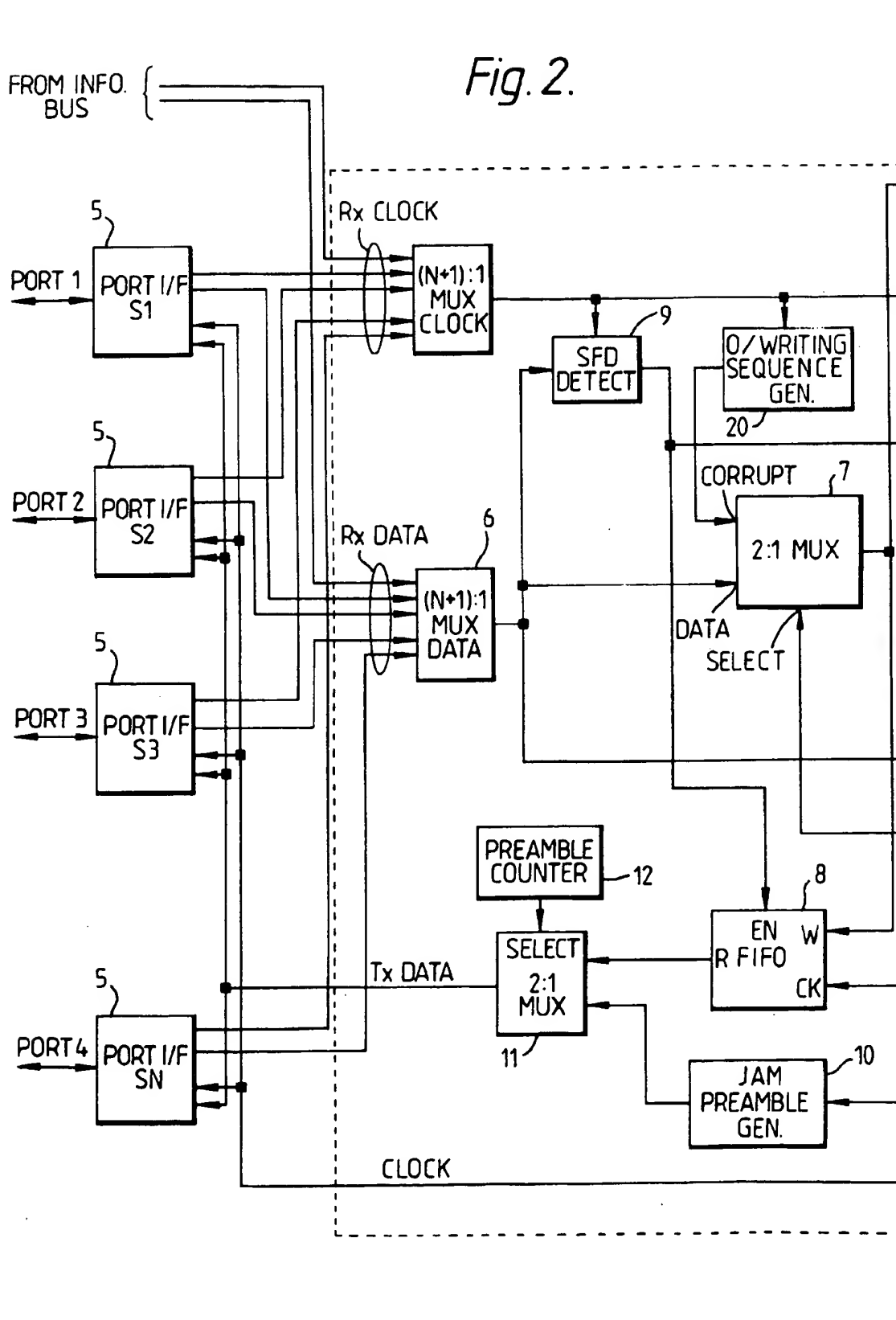


Fig. 2(cont.)

